ABSTRACT

In a tree-structural key distribution system, renewed data of a master key and medium key are sent along with a key renewal block (KRB). KRB is such that each of devices included as leaves of a tree structure has a leaf key and restricted node key. A specific KRB can be generated for a group identified by a specific node and distributed to the group to restrict a device for which the key can be renewed. Any device not belonging to the group cannot decrypt the key, whereby the security of key distribution can be assured. Especially in a system using a generation-managed master key, a master key renewed with KRB can be distributed.